

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Previously Presented) An information recording device for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording device comprising:

a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors;

wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

Claims 2-4 (Canceled).

5. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector

is executed as single-DES encryption processing using different encryption keys for the sectors.

6. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors.

Claim 7 (Canceled).

8. (Previously Presented) An information playback device for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number said information playback device comprising:

a cryptosystem unit which selectively uses a different decryption key for each sector from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on data stored in each of the sectors;

wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

Claims 9-11 (Canceled).

12. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors.

13. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at least two different decryption keys for each of the sectors.

Claim 14 (Canceled).

15. (Previously Presented) An information recording medium having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number,

wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area,

wherein the storage area stores data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information, and wherein an integrity check of the integrity of the revocation list and block permission table is performed.

16. (Original) An information recording medium according to claim 15, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors.

17. (Previously Presented) An information recording method for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording method comprising:

 encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector;

 storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

 performing an integrity check of the revocation list and the block permission table.

Claims 18-20 (Canceled).

21. (Previously Presented) An information recording method according to claim 17, wherein the encryption processing is executed as single-DES encryption processing using different encryption keys for the sectors.

22. (Previously Presented) An information recording method according to claim 17, wherein the encryption processing is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors.

Claim 23 (Canceled).

24. (Previously Presented) An information playback method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information playback method comprising:

decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

performing an integrity check of the revocation list and the block permission table.

Claims 25-27 (Canceled).

28. (Previously Presented) An information playback method according to claim 24, wherein the decryption processing is executed as single-DES decryption processing using different decryption keys for the sectors.

29. (Previously Presented) An information playback method according to claim 24, wherein the decryption processing is executed as triple-DES decryption processing using at least two decryption keys for each of the sectors.

Claim 30 (Canceled).

31. (Previously Presented) A computer-readable medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising:

storing data in a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number;

encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector; storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and checking the integrity of the revocation list and the block permission table.

32. (Previously Presented) A computer readable medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising:

reading data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number;

decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

checking the integrity of the revocation list and the block permission table.